# Attachment A

## TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

## PHASE III - PROTOTYPE PHASE

## REQUIREMENTS DOCUMENT

# *1 TWIC Program Overview*

## *1.1 Mission*

1.1.1 The mission of the Transportation Worker Identification Credential (TWIC) program is to design and field a common credential or standard for all transportation workers requiring unescorted physical and logical access to secure areas of the national transportation system. In achieving the TWIC Program's mission, three overarching goals must also be achieved:

- Improve security;
- Enhance commerce; and,
- Protect personal privacy

1.1.2 When fully implemented, the TWIC program may issue credentials to up to 6 million transportation workers or provide a standard that could be used by companies/facilities that require employees to have access to secure areas. TSA can only estimate the population at this time because definitions of secure areas have not been developed or finalized in all modes of transportation. Further, states may establish their own transportation credentialing requirements that may take the place of Federal requirements. As population estimates are refined, the TWIC Program will adjust its analysis and planning as appropriate. TWIC holders will be positively matched to a credential and a successfully completed background check via a reference biometric.

1.1.3 The TWIC will be designed to help integrate existing identity management and access control capabilities so that any solution will be interoperable among each mode of transportation.

1.1.4 The TWIC program consists of five phases: Phase I—Planning, Phase II—Technology Evaluation, Phase III—Prototype, Phase IV—Implementation, and Phase V—Operations and Maintenance. This document addresses Phase III Prototype objectives and system requirements.

### *1.2 Overall Program Objectives*

1.2.1 Develop a common credential or standard, universally recognized and accepted across all modes of the transportation system, funded primarily by user fees, as is the case in other modes of transportation.

1.2.2 Create a uniform, nationwide standard for secure identification of transportation workers.

1.2.3 Minimize the requirement for redundant credentials and background checks.

1.2.4 Design a solution to positively and securely link an individual to her credential via a reference biometric and to the background information on the claimed identity of that individual.

1.2.5 Ensure that the TWIC solution is compatible with existing facility access control and related systems to leverage current security investments.

1.2.6 Ensure the ability to quickly revoke access privileges to TWIC holders who are identified as a threat after issuance of their credentials, and immediately remove lost, stolen, or compromised cards.

# *2 Phase III – Prototype Phase Overview*

## *2.1 Purpose*

2.1.1 Evaluate the utility of the TWIC integrated solution and detect and resolve weaknesses before proceeding to Implementation Phase. Test infrastructure necessary to proceed to Implementation Phase.

## *2.2 Scope*

2.2.1 Participation in Prototype will be supported by transportation facilities located in each of the following regions:

*2.2.1.1 East- Delaware River and Bay and Long Island, NY (Islip airport)*

*2.2.1.2 West - Los Angeles / Long Beach and Port of Oakland*

*2.2.1.3 Florida – State's 14 deepwater ports and Florida Department of Highway Safety and Motor Vehicles*

2.2.2 The participating facilities may include a variety of transportation modes, to include Rail, Pipeline, Maritime, Trucking, Mass Transit, and Aviation. Total estimated population will not exceed 200,000. A Prototype Site Matrix is provided at Attachment B for additional details.

2.2.3 The following high-level business processes and capabilities represent the Prototype scope:

*2.2.3.1 Employer/entity registration*

*2.2.3.2 Applicant Processing*

*2.2.3.3 Claimed identity validation*

*2.2.3.4 Enrollment Center Processing*

*2.2.3.5 Fee collection (note: The Federal Government does not currently have the regulatory framework in place to collect fees; however, the State of Florida may collect fees during performance of Phase III in accordance with Florida law)*

*2.2.3.6 Biometrics (reference and operational)*

*2.2.3.7 Biometric check (1:N) against the ID Management System (IDMS)*

*2.2.3.8 Fingerprint-based Background Check Interface (Florida only)*

*2.2.3.9 Name-based threat assessment~~background checks~~*

*2.2.3.10 Card production and personalization*

*2.2.3.11 Card/Token Management System*

*2.2.3.12 Issuance/Re-issuance*

*2.2.3.13 Adjudication*

*2.2.3.14 Card Activation*

*2.2.3.15 Privilege granting at local facility TWIC node*

*2.2.3.16 Interfaces between specified Access Control Systems and TWIC Local Node ~~IDMS~~*

*2.2.3.17 Revocation processes*

*2.2.3.18 Prototype system auditing, monitoring and evaluation methodologies*

*2.2.3.19 System Administration and System Maintenance functions*

*2.2.3.20 Help Desk*

*2.2.3.21 Installation, training, operations, and reporting*

## *2.3 Prototype Goals*

2.3.1 The Prototype Phase will assess feasibility of potential Implementation phase requirements. Prototype provides an experiential opportunity for a solution to operate with live systems, implemented in a variety of transportation facility environments. Prototype should assess feasibility of varying foundations upon which a full-scale Implementation could proceed.

## *2.4 Assumptions*

2.4.1 Card production and capabilities will be provided as Government Furnished Property (GFP); however, the Contractor must provide card stock.

2.4.2 Following Prototype, many facilities will rely on the TWIC as a "flash-pass" until such time as necessary investment capital is available to purchase infrastructure and/or access control systems.

2.4.3 The Department of Highway Safety and Motor Vehicles (DHSMV) will provide the Florida Master Access Control Database; therefore, Offerors should consider this database as GFP.

2.4.4 Contractor will be required to provide labor support at enrollment centers for duration of Prototype.

2.4.5 Communications infrastructure at local facilities may range from dial-up to robust T-1/3 lines.

2.4.6 The enrollment process may take place in a variety of locations, including Federal, state and local government as well as private industry facilities.

2.4.7 Primavera/TeamPlay® will be used by the government to track Prototype activities, including cost, schedule, performance, issues, and any deviations between planned and actual data.

2.4.8 Prototype will be a highly collaborative process among contractor, government, and stakeholders.

2.4.9 Florida will use existing live scan devices (CrossMatch®) to collect 10-print images for processing through the Florida Department of Law Enforcement (FDLE).

2.4.10 The government will furnish a list of documentation to be considered by the Offerors to help establish and verify an applicant's claimed identity.

2.4.11 Government stakeholder and technical representatives will accompany the contractor on any site survey teams.

2.4.12 It is anticipated that not all TWIC applicants will have an employer per se; therefore, the Offeror should assume that the port or transportation facility may serve as their sponsor.

2.4.13 Federal central card personalization facility will inspect, store, and track cards upon receipt.

2.4.14 The reference material provided by the government represent TWIC Prototype Phase requirements

### *2.5 Reference Material*

2.5.1 *(Reserved)* (Attachment A)

2.5.2 Prototype Site Matrix (Attachment B)

2.5.3 TWIC Data Requirements (Attachment C)

2.5.4 System Concept of Operations (Attachment D)

2.5.5 Functional Requirements Document (Attachment E)

2.5.6 TWIC Topology and Biometric Document (Attachment F)

2.5.7 Florida Processes and Requirements Document (Attachment G)

2.5.8 Florida Site Matrix (Attachment H)

2.5.9 TWIC Conceptual Architecture (Attachment I)

2.5.10 Technology Evaluation Phase Government Furnished Equipment (GFE) (Attachment J)

2.5.11 Claimed Identity Working Group Final Report (Attachment K)

*(Note: The government will provide the latest copies of these and other documents at contract award.)*

## *3 Prototype Requirements*

### *3.1 Identification Management System*

3.1.1 The proposed solution must demonstrate a central database with minimum data to enable streamlined operations, protect personal privacy, and to maintain a chain of trust.

3.1.2 The system must have the capability to securely segment and protect the full enrollment dataset from the minimal IDMS record.

3.1.3 The storage solution must include provisions for disaster recovery and continuity of operations, consistent with the scope and scale of Prototype.

3.1.4 The system must provide a secure and reliable storage platform for retaining biographic and biometric information.

3.1.5 The information must remain online to ensure fast access to the information and make provisions for the following attributes:

*3.1.5.1 Content integrity*

*3.1.5.2 Content authenticity*

*3.1.5.3 Guaranteed record retention period (SEC regulation 17a-4)*

*3.1.5.4 Provisions for content shredding (e.g., DOD 5015.2)*

*3.1.5.5 High Availability Features*

*3.1.5.6 Content mirroring*

*3.1.5.7 Local and remote replication*

### *3.2 Information Collection / Capture*

3.2.1 The solution must have the capability to capture unstructured data (i.e. biometric information, birth certificate, driver's license, green card, application, etc.); encrypt data; digitally sign information with signature of enrollment officer; store locally, and securely transmit to TSA.

### *3.3 Information Distribution / Aggregation*

3.3.1 The solution's data distribution (one to many model) must push identity management information to the field.

3.3.2 The solution's data aggregation (many to one model) must pull security log and enrollment information from the field for analysis

3.3.3 The solution must be capable of encrypting and compressing data, and scheduling data transfer using rules-based processes

3.3.4 The solution must be capable of transferring data, and providing the following capabilities:
*3.3.4.1 Retry on failure or interruption*
*3.3.4.2 Check pointing during transfer – incremental retransmit*
*3.3.4.3 Data transfer logging and notification*

### *3.4 Database Scalability*

3.4.1 The proposed database technology must accommodate a minimum of 6 million cardholder records with a capability for growth, scalable to 10 million.

### *3.5 Data and Document Storage, Retention and Archiving*

3.5.1 The proposed solution must provide a data interface for the secure transfer of enrollment data between enrollment centers, local TWIC node, background check process, terrorist screening system, the IDMS, and card production facility.

3.5.2 The proposed solution must support a rigorous audit and inspection process. It must include remote electronic audit capability and an overall audit process.

3.5.3 The solution must include an alerting/reporting mechanism that is triggered for specified events or activities within the IDMS. Examples include, but are not limited to:

*3.5.3.1 Cards issued, but never activated or registered for access at a transportation facility*

*3.5.3.2 Applicants who have not received their cards within appropriate time standards*

*3.5.3.3 Change in cardholder information over time that may now represent an unreasonable security risk*

*3.5.3.4 Cards shipped from card production facility, but with no record of receipt at enrollment center*

### *3.6 Availability*

3.6.1 The solution will include appropriate provisions for redundant hardware, off-line operations capability, disaster recovery, and business continuity measures.

3.6.2 The system must include a power backup that ensures data is retained in event of power loss.

3.6.3 The TWIC fixed base and mobile readers should operate from line power (US and international), automotive electrical systems, or interchangeable rechargeable battery pack as appropriate.

3.6.4 Mobile device battery life should be at least 10 hours under constant usage.

3.6.5 Database availability will be 99.99 %.

### *3.7 Interoperability*

3.7.1 Solution should be interoperable with existing Federal credentialing systems, using the GSC-IS interoperability specification.

3.7.2 The solution should minimize local facility investments by leveraging, maximizing, and/or interfacing with existing physical access control infrastructures.

3.7.3 Biometric solutions should be, to the maximum extent, compatible with related DHS and Federal programs.

3.7.4 Solution must be interoperable with card readers, sensors, and systems among the prototype regions and locations. Specifically, cards issued/activated at any TWIC Prototype location, and procured as a part of this effort must work with another facility's reader, subject to the local facility authorizing/granting the access, and consistent with the technologies employed.

3.7.5 The solution must include an approach to developing and providing a 'Compatible Products' list that could be used by stakeholders to help ensure products being considered for procurement are compatible with the TWIC solution.

### *3.8 Enterprise Architecture*

3.8.1 The Prototype solution must be based on an open architecture that complies with the established Federal Enterprise Architecture (http://www.feapmo.gov) and applicable TSA standards.

3.8.2 Standard and open communication protocols should be used.

3.8.3 The solution should include provisions for disaster recovery, continuity of operations, and protecting personal privacy in accordance with applicable law to include The Privacy Act of 1974, 5 U.S.C. § 552a.

### *3.9 Standards (as applicable)*

3.9.1 National Institute of Science and Technology (NIST).

3.9.2 Federal Information Processing Standards 140.

3.9.3 Government Smart Card Interoperability Specification, v2.1 or higher.

3.9.4 International Organization for Standardization (e.g. ISO 7810, 7816, 14443, 15693, etc.).

3.9.5 Security Equipment Integration Working Group (SEIWG 012).

3.9.6 Global Platform.

3.9.7 American National Standards Institute/International Committee on Information Technology Standards (ANSI/INCITS) (i.e., INCITS 383)

### *3.10 Durability*

3.10.1 The lifecycle goal of the credential is 5 years of operational use.

3.10.2 Any contact or contactless solution, and the technologies it houses, will survive normal wear and tear consistent with ISO standards and industry best practices.

3.10.3 The fixed base and mobile readers should have a minimum 10,000-hour Mean Time Between Failure.

### *3.11 Interface Requirements*

3.11.1 Solution interfaces must use open industry standards for all TWIC equipment.

3.11.2 Interfaces that are a part of the solution must be documented, and include sufficient details of the interfaces, including, but not limited to, card readers, workstations, and Local Area Network connections.

3.11.3 At a minimum, the proposed solution should support Ethernet 10/100 and WiFI 802.11B/G interfaces.

3.11.4 The solution must be capable of facilitating the transfer, in single or batch, valid TWIC holders, to the local facility's access control system. This capability must ensure and maintain the integrity, trust, security, and performance of the solution.

3.11.5 The solution must be capable of accepting an import of workers who have already completed a background check, subject to data verification/validation.

3.11.6 The solution must include the ability to securely receive and transmit data elements between the enrollment centers, appropriate databases, local TWIC node, IDMS, and government-specified Access Control Systems.

3.11.7 The solution may be required to interface with a future TSA Credentialing Program Office (CPO)-developed technology platform used to conduct name-based terrorist threat assessments on TWIC prototype participants. This technology platform is currently in the planning phase.

### *3.12 Reading/Verification Speed and Reliability*

3.12.1 The prototype credential data storage elements (ICC, barcode) should support data interrogation within one-half (0.5) second, enabling the find, decode and display of stored and/or encoded card information on fixed and mobile devices within one (1) second after the credential is interrogated.

3.12.2 When reference or operational biometric data is read, the fixed base or mobile device should support biometric verification within two seconds of credential interrogation.

3.12.3 The TWIC should be capable of 99.99% data read accuracy. Biometric matching should have accuracy of 99% or higher. The biometric Equal Error Rate (ERR) should be not more than 1%.

3.12.4 Mobile and fixed base devices should accurately interrogate the TWIC 99.99% of the time on the first attempt.

3.12.5 When a reference or operational biometric verification (1:1) is initiated, the correct result (accept or decline) should be accomplished on the first attempt at least 90% of the time.

3.12.6 The overall credential failure/replacement rate objective is 2%.

### *3.13 Card and Card Security*

3.13.1 The solution must include the use and evaluation of the iris as the system's reference biometric at one prototype location. The government anticipates the use of the iris as the reference biometric will be in addition to use of a fingerprint biometric at the designated facility.

3.13.2 The solution must use appropriate visible and invisible card security measures for the baseline prototype credential as specified in Attachment F.

*3.13.2.1 Visible anti-counterfeiting features such as fine line Guilloche background printing, laser engraving, ghost portraits, altered font, holograms, kinegrams, tri-color laminate, etc. may be considered.*

*3.13.2.2 The card should contain covert security features. These covert features would include digital watermarking, UV ghost images, and full color UV.*

3.13.3 Portable and fixed base readers should have the ability to view and confirm selected anti-counterfeiting techniques.

3.13.4 The card will be designed to minimize the ability to physically alter the card and its media for the purpose of unauthorized use, including unauthorized physical or logical access.

3.13.5 The card will not be easily duplicated, nor will the inherent security features on the card be by-passable by unauthorized personnel.

3.13.6 All cryptographic functions must be performed on the card to prevent private keys and other critical data from being covertly copied or compromised.

3.13.7 The solution must use a standards-based authentication method, and the card authentication protocol shall conform to open protocol standards.

3.13.8 The baseline prototype credential shall be a standard contact and/or contactless card. The government anticipates that a majority of prototype credentials will be contactless.

3.13.9 The solution must include provisions for a variety of media and technologies, to include proximity and optical memory

3.13.10 The card should be constructed to support a minimum of 5 years of use in transportation system conditions with appropriate care.

### *3.14 On Card Storage*

3.14.1 The ICC (contact or contactless) on the card will be able to store keys and certificates to perform necessary encryption and digital signature functions for authentication of personal identity and applicable information.

3.14.2 The solution must have the ability to store, retrieve, and use an operational biometric on the ICC.

### *3.15 Information Assurance and Access*

3.15.1 The solution must be capable of supporting information assurance (IA) requirements to access sensitive but unclassified information and equipment, such as telephone, computers, Personal Data Assistants (PDAs), and other mobile or portable devices.

3.15.2 The solution must act as a hardware token, containing private keys and certificates for authentication, digital signature, and e-mail encryption/ decryption capabilities to enable the user to securely access networks, computer systems, and applications.

3.15.3 The solution must support logical access to networks, including Local Area Networks (LAN), Wide Area Networks (WAN) and information systems configured to require authentication via public key technology.

3.15.4 Enrollment software must have the capability to provide an expiration date and/or a minimum frequency-of-use period for cards.

3.15.5 All enterprise transport must be protected using appropriate levels of security.

### *3.16 Performance Parameters*

3.16.1 The solution must be capable of providing, tracking, reporting performance metrics for the Prototype solution. The collected metrics must be actionable and help improve the system's operational performance, security, utility, cost, or ease of use.

3.16.2 During the execution of Prototype, local facility card to reader credential validation transaction times as well as any enterprise database transactions must be recorded and evaluated. Transaction times shall be measured from presentation of the card to the reader, comparison to any required local or remote data elements, and positive verification of cardholder identity.

3.16.3 The solution shall maintain average enrollment transaction time of not more than 10 minutes for initial enrollees, not more than 8 minutes for replacement cards, and not more than 2 minutes to validate identity and activate / issue the TWIC when it arrives from the production center.

3.16.4 The solution must be capable of collecting and analyzing enrollment fee collection times and payment details.
*3.16.4.1 Note: The Federal Government does not currently have the regulatory framework in place to collect fees; however, the State of Florida may collect fees during performance of Phase III in accordance with Florida law*

3.16.5 The system shall be capable of measuring overall lost card rates and turnover rates, as well as rates within target populations.

3.16.6 The system shall be capable of recording the time required to adjudicate biometric matches.

3.16.7 The system shall be capable of recording the percentage of records requiring adjudication. Software shall yield less than 7% match rate at database populations of 3 million records. (Note: This minimum performance threshold applies to generation of candidate lists that require adjudication.)

3.16.8 Enrollment center processing time for lost, stolen or re-issued cards shall be recorded and analyzed.

3.16.9 Elapsed time for enrollee to pick up card after notification of credential production shall be recorded.

3.16.10 The system shall be capable of collecting and reporting the following metrics, at a minimum, on a weekly basis:

*3.16.10.1 Number of TWICs requested*
*3.16.10.2 Number of TWICs issued*
*3.16.10.3 Number of, and reason for cards rejected and/or not issued*
*3.16.10.4 Average enrollment time per TWIC*

3.16.11 Transaction times for 1:1 biometric matches during the card issuance process shall be recorded.

3.16.12 The solution shall be capable of generating reports on the data currency and providing notifications if the currency of TWIC data is outside of acceptable thresholds.

***3.17 Prototype Report. The Contractor will prepare a Prototype Report that compares the Prototype Phase performance and activities against the TWIC Program goals, objectives, and requirements. The report should include, but is not limited to, lessons-learned from the Prototype Phase, results of performance metrics, and recommendations that serve to facilitate decision making and future implementation decisions and related considerations. The Prototype Report will be a comprehensive and collaborative effort, which will include inputs from the prime vendor, management support staff, integrated project team members, stakeholders, and an independent verification/validation (IV&V) contractor. The Prototype Report must include the following:***

3.17.1 Identity Verification (Identity Authentication)
*3.17.1.1 Percentage per type of breeder document presented at enrollment center location*
*3.17.1.2 Counterfeit documents detected*
*3.17.1.3 Supervisor interventions*

3.17.2 Enrollment (Background Check)
*3.17.2.1 Transaction times*
*3.17.2.2 Percentage using web-based pre-enrollment*
*3.17.2.3 Supervisor interventions*

3.17.3 Card Production (Identity Token)
*3.17.3.1 Cards produced per hour*
*3.17.3.2 Cost per card*
*3.17.3.3 Failure and reject rates*

3.17.4 Biometrics (Identity Verification)
*3.17.4.1 Failures per enrollment attempt*
*3.17.4.2 Failure to Acquire*
*3.17.4.3 Failure to Enroll*
*3.17.4.4 False reject rate*
*3.17.4.5 False accept rate*

3.17.5 Secure Areas (Access Control System, Access Control Points, and Revocation)
*3.17.5.1 Access transaction times for personnel and vehicles*
*3.17.5.2 Intrusion attempts*
*3.17.5.3 Mean-time-between-failure rates*
*3.17.5.4 Scheduled-unscheduled maintenance rates*

3.17.6 Cost/benefit analysis of contact and contactless (including proximity) cards

3.17.7 Analysis of iris-based biometric as a reference biometric

3.17.8 Estimated costs of system and components to federal government

3.17.9 Estimated costs of system and/or components to each facility owner

3.17.10 Document the effects the system has on security (e.g., local, regional, and national levels)

### *3.18 Standard Operating Procedures*

3.18.1 The solution must include documented Standard Operating Procedures (SOPs) that are tailored for the roles and responsibilities of TWIC user classes and appropriate functional activities (e.g., pre-enrollment, enrollment, revocation, etc).

### *3.19 Pre-Enrollment*

3.19.1 The solution must be capable of pre-enrollment processes and payment functions

3.19.2 The solution must incorporate the use of unmanned kiosks that applicants can use to pre-enroll.

3.19.3 The solution must include a multi-lingual (English/Spanish) pre-enrollment (hard-copy) application for enrollment purposes

### *3.20 Enrollment*

3.20.1 The solution must include an enrollment center with one or more enrollment-station(s) that possesses the ability to perform all enrollment functions, to include:

*3.20.1.1 Retrieval of pre-enrollment employer sponsorship, biographic, and payment information*

*3.20.1.2 Support the claimed identity verification process*

*3.20.1.3 Capture biographic and biometric data for initiation of a background check and TWIC registration processes*

*3.20.1.4 Image-capture, verification and retention of claimed ID documents*

3.20.2 The enrollment solution must minimize manual data entry of initial biographic and demographic information.

3.20.3 The solution should define recommended enrollment center considerations such as physical and information security, protecting personal privacy, photographic standard, background color, and other appropriate instructions. This information must be included in standard operating procedures.

3.20.4 The solution must include a capability for conducting a high volume of enrollments in a short amount of time during initial issuance at local facilities.

### *3.21 Schedule / Appointment Capability*

3.21.1 The solution must include an appointment scheduling and management tool for use by applicants, employers, enrollment center clerks, and other appropriate personnel.

### *3.22 Training and Certification*

3.22.1 The solution must include a training program for individuals who will operate and supervise the Enrollment Center equipment, and a certification program for both the site and individuals. The training program must help ensure trust and authenticity of enrollment center activities and transactions, and mitigate risk of fraudulent activities.

3.22.2 The tool must include a tutorial, template for biographic data, help function, and be able to designate/select the enrollment center to be used by the employee and provide the option to schedule appointments.

### *3.23 Claimed Identity*

3.23.1 The solution must include the ability to assist the enrollment clerk in determining the authenticity and accuracy of claimed identity or "breeder" documents (see attachment K)

3.23.2 The solution must have the ability to inspect and scan identification materials presented for inclusion into the enrollment record.

### *3.24 Security Features*

3.24.1 The solution must include an enrollment station that has high-level security measures to protect the integrity and privacy of TWIC data.

*3.24.1.1 Possible security features include but are not limited to a positive verification of the identity and permissions of the authorized operator (TWIC and biometric match), anti-tamper features, capability to encrypt data transmissions, and support for an audit/logging system.*

3.24.2 The solution must permit the Trusted Agent at the enrollment center to digitally sign each enrollment record and transaction generated to ensure authenticity.

3.24.3 System must be designed with the ability to grant specific privileges to specific individuals based on job requirements, duties, or roles.

### *3.25 Fee Collection*

3.25.1 The solution must have the capability to collect and process a fee for service. The fee may be collected via electronic transactions, credit cards, and cash, checks and/or money orders.
*3.25.1.1 Note: The Federal Government does not currently have the regulatory framework in place to collect fees; however, the State of Florida may collect fees during performance of Phase III in accordance with Florida law*

### *3.26 Employer/Employing Entity Registration*

3.26.1 The solution must include a standard process to register employers and establish a link between them and the TWIC applicants they sponsor. This includes the functionality for an employer to be able to batch transfer employee information to pre-populate the enrollment record.

3.26.2 The solution should demonstrate alignment with current federal cross-credentialing concepts and trust models.

### *3.27 Issuance Components*

3.27.1 The solution must integrate with appropriate components of the Card Management System (CMS) to ensure a secure and integrated life cycle for card and card components.

3.27.2 The solution must include a process for the identification and elimination of faulty cards and establish a quality assurance process to validate card accuracy. The Offeror's solution must include the capability to create / obtain failure analysis reports as requested.

3.27.3 The solution must include a plan to integrate central card production with components of the proposed solution.

3.27.4 The solution must include a security model for the card that is consistent with the overall security requirements and operational environment for the solution. The security model must be compliant with GSC-IS and appropriate FIPS-140 requirements and standards, as applicable.

3.27.5 The solution must include a biometric capability with the card consistent with the TWIC Biometric and Topology Document (Appendix F).

### *3.28 Credential Revocation / Re-Issuance*

3.28.1 The solution must include a process to accept and document the report of lost, stolen, and damaged cards, accept their return, and initiate a replacement card transaction with proper notifications, audits and updates to IDMS, the Card Management System, and other appropriate data sources or systems.

*3.28.1.1 Specific revocation and re-issuance requirements are documented in the Functional Requirements Document (FRD) (Attachment E).*

### *3.29 Privilege Granting Component (TWIC Local Node)*

3.29.1 The system shall support a TWIC local facility node that will receive and transmit information from/to the IDMS.

3.29.2 The local TWIC node must have connectivity to allow the processing of TWIC hot-list data and downloading specific updates, alerts, and information to/from the IDMS database.

3.29.3 The local TWIC node must be capable of interacting with local access control systems.

3.29.4 The TWIC local node should minimize physical footprint due to space limitations at local facilities.

### *3.30 System Administration Components*

3.30.1 Audit Program. The solution must support a rigorous audit and inspection process. The solution must include remote electronic audit capability and an overall audit process.

3.30.2 The solution must specify, document, and include an appropriate and secure storage solution for TWICs awaiting issue or collection.

3.30.3 Disposition. The solution must include a methodology to appropriately dispose of TWICs deemed non-operational, and this methodology must be included in an SOP.

3.30.4 Role-based responsibilities. The solution must include a role-based approach to ensure accountability and trust of enrollment processes and personnel (e.g., use of a two-person rule), and include these responsibilities in applicable SOPs.

### *3.31 Florida Requirements*

3.31.1 Known Florida processes and requirements are included in Attachment G.

3.31.2 The solution must comply with all applicable laws, both State and Federal, but in the event of a conflict, Federal law will govern.

### *3.32 Help Desk*

3.32.1 The solution must include 24/7 technical support

3.32.2 The solution must include on-site technical support during installation and training.

3.32.3 The solution must include appropriate warranty and maintenance service for all procured, installed, or supported components, and this information must be documented in local facility Standard Operating Procedures.

### *3.33 Audit*

3.33.1 The system should record appropriate events to help ensure accountability and validity of actions in the enrollment process and to mitigate security risks.

3.33.2 The system must include the capability to broadcast and/or otherwise providing time-sensitive information, such as notices of revoked, or hot-listed cards, alerts, to local facilities (via TWIC local node).

### *3.34 Connectivity*

3.34.1 The solution must be capable of many types of secure connectivity at facilities including: dedicated connections, broadband Digital Subscriber Line (DSL) and cable modem services, analog modem, and wireless data access.

3.34.2 The solution may include required connectivity independent of communications infrastructure at local facilities.

### *3.35 Safeguarding Information*

3.35.1 The Contractor shall take all appropriate measures to ensure that information provided by the Government is properly safeguarded in accordance with applicable law to include the Privacy Act of 1974, 5 U.S.C. § 552a.

3.35.2 The Contractor shall not provide the data to any other government or non-government agency without the express written permission of TSA unless such data is compelled by judicial or administrative proceedings.

3.35.3 The Contractor shall avoid such disclosure and shall afford the Government the opportunity to obtain assurance that compelled disclosure will receive confidential treatment.

3.35.4 The Contractor shall not use the data in any other contract, test or application other than those specifically authorized by TSA.

3.35.5 The Contractor shall not seek financial gain (other than the contract itself) through its use of the data to include advertising or indicating to government or non government activities that it uses the data in the execution of its contract.

3.35.6 The Contractor shall not publicize the specific nature of its use of the data to anyone outside of TSA.

## *3.36 Evaluation of Additional Identity Management Components*

3.36.1 The purpose of Prototype Phase is to evaluate the full range of Identity Management business and security processes. The preceding portions of Section 3, Prototype Requirements, provide detail on one complete set of identity management components, which constitute the baseline commonly referred to as the TWIC System. In addition to the Prototype Report mentioned in section 3.17, interim data will be gathered and periodically analyzed. To achieve the complete evaluation goal, the government reserves the right to evaluate additional Identity Management components either individually or in selected combinations.

3.36.2 As a part of the contractor's proposed solution, and in a phased approach, the contractor shall provide for the evaluation of the components below. This evaluation will be conducted by comparing the baseline with the alternatives expressed below. The following components represent the key areas for evaluation:

*3.36.2.1 Identity Verification:*

- TWIC System baseline: An in-person transaction where a range of breeder documents are examined and accepted by a trusted agent to establish the baseline identity. The results are documented and retained in the Identity Management System (IDMS). The verified identity is then used to conduct the appropriate background check.
- Alternative A: Evaluate use of the results from a third party with an independently developed process, e.g. representative of current industry practices
- Alternative B: Evaluate use of the results from a third party's compliance with a specifically designated federally approved process (e.g., Aviation's Secure Identification Display Area (SIDA)) practices.

*3.36.2.2 Identity Authentication:*

- TWIC System baseline: The foundation for future identity authentication is established by collecting a reference biometric at the time of identity verification. This biometric is used to prevent fraudulent, alias, or dual registrations, as well as to permanently and positively link the individual, via biometric, to the verified identity and background check. The results are documented, maintained, and managed within the IDMS.
- Alternative A: Evaluate the use of a third party process that reflects current industry practices (e.g., accept a common third party document like a state driver's license to provide the link).
- Alternative B: Evaluate the use of a specifically designed process that issues a basic identification card (e.g., "flash-pass" or photo ID) to establish the link or relationship.

*3.36.2.3 Background Check*

- TWIC System baseline. Consists of both criminal records history check and terrorist threat assessment. Each would be periodically updated to ensure both accuracy and data currency. The checks are conducted only upon verified identities with enrollment records.
- Alternative: Conduct the appropriate background check one time, without the requisite enrollment record.

*3.36.2.4 Identity Token*

- TWIC System baseline: Using a secure process, the appropriate token (in accordance with OMB policy direction regarding smart cards systems for identification and credentialing, dated February 2004), a smart card based credential that conforms to federal GSC-IS specification is centrally produced and personalized, and issued to the individual. The issuance is documented and the token lifecycle is managed within IDMS. The token is used, across the transportation system, to authenticate identity, document the baseline background check and link with updated background information that is disseminated via the IDMS.
- Alternative: Evaluate the use of the token's other surface based technologies, e.g., without the biometric data on the ICC, or another token's surface based technologies in the same role as the baseline process.

*3.36.2.5 Access Control System and Access Control Points*

- Note: Access control systems and access control points are a local facility and industry responsibility. In order to properly support the prototype evaluation and to evaluate crucial interoperability requirements, selected prototype sites will have temporary modifications or improvements to current system capabilities.
- TWIC System baseline: The government will make selected investments at local facilities in temporary modifications and improvements to gather minimum data to support prototype evaluation at a range of modes, facilities and worker types. The TWIC will be evaluated using the token's primary and other surface based

technologies with a full range of legacy systems and with any temporary modifications required to support the evaluation.
- Alternative: Evaluate the TWIC and other tokens with existing access control points and systems.

*3.36.2.6 Revocation*

- Note: By the nature of the industry, the personnel in the transportation system are mobile. Many individuals have duties at multiple facilities in various locations. Timely dissemination of updated threat information or possible fraudulent activity is required to complete the security chain of trust.
- TWIC System baseline: Evaluate a range of revocation response methods and times that meet the appropriate industry security plans and requirements, and DHS approved security plans.
- Alternative A: Evaluate use of third party or indirect revocation.
- Alternative B: Evaluate a system without revocation.

3.36.3 The Prototype Phase will include three separate regions with a range of local facilities that vary by transportation mode (e.g., maritime, airport, rail, pipeline, transit, truck, etc.), category of worker (e.g., management, labor, driver, laborer, etc.), size, sophistication of business operation, organizational relationships, governance and regulation, current investment in security, etc. The evaluation of the TWIC baseline and the combinations or alternative elements will be phased-in, with respect to time, components, and location. This is required by evaluation standards for separation and fairness, and the need to provide business operation flexibility to our voluntary prototype partners. The government will provide a detailed planning matrix, that includes the schedule, location; timing and specific activity for the evaluation of these components will be developed in conjunction with the draft prototype evaluation.

## *4 Management Processes*

### *4.1 Integrated Project Team (IPT) Functions*

4.1.1 The TWIC Program has established IPTs to coordinate activities within each region. The selected Offeror will be an integral part of these IPTs. Contractors are expected to actively participate as members of their respective IPT and take direction from the Government IPT leads. Government IPT leads will be the communication conduit between local facilities and TWIC Program office. Contractor communication will be required with the TSA Credentialing Program Office (CPO) for purposes of discussing background checks, threat assessments, and hazardous material endorsements on Commercial Drivers Licenses. It is anticipated that IPTs will be composed of the following groups:

*4.1.1.1 TSA Credentialing Program Office (CPO)*

*4.1.1.2 TWIC Program Office*

*4.1.1.3 Bureau of Customs and Immigration Services (BCIS)*

*4.1.1.4 Florida Department of Highway Safety and Motor Vehicles (DHSMV)*

*4.1.1.5 TSA Chief Information Officer (CIO)*

*4.1.1.6 TSA IT Managed Services (ITMS) Contractor*

*4.1.1.7 TSA Chief Information Security Officer*

*4.1.1.8 TSA Chief Technology Officer (i.e., TSA Technology Center, Operational Integration, and Independent Verification/Validation Contractor)*

*4.1.1.9 Prototype Contractor*

*4.1.1.10 Stakeholders (internal/external)*

*4.1.1.11 TSA Contracting Officer*

*4.1.1.12 Contracting Officer's Representative (COTR): The COTR is a TWIC program official who is designated by the Contracting Officer (CO) to assist in administering the contract or task order. The COTR should provide technical information, and, as appropriate, technical direction, with respect to the specifications or work statement, and will monitor, inspect, accept/reject, and or make recommendations to the Offeror's progress and performance. All decision related correspondence between the Offeror and the TWIC Program Office should either be directed to or copied to the COTR. Please also note that the COTR does not have the authority to take any action, directly or indirectly, that will change the pricing, quantity or delivery schedule, nor can the COTR direct the accomplishment of effort that goes beyond the scope of the contract or task order.*

4.1.2 The IPTs provide a wide range of functions including but not limited to:

*4.1.2.1 Management and facilitation of all TWIC related activities for the region*

*4.1.2.2 Coordinating stakeholder activities*

*4.1.2.3 Coordinating and conducting site surveys*

*4.1.2.4 Conducting site visits*

*4.1.2.5 Managing stakeholder relations*

*4.1.2.6 Resolving TWIC related issues*

*4.1.2.7 Identifying and forwarding to headquarters any policy concerns/issues*

*4.1.2.8 Identifying and addressing TWIC Business Processes*

### *4.2 Site Surveys*

4.2.1 The schedule objective is to commence site surveys within 15 days of Contract Award.

4.2.2 The contractor will conduct site surveys at all prototype locations and should recommend an approach to deployment and integration that emphasizes speed and quality.

4.2.3 Government stakeholder and technical representatives will accompany the contractor on any site survey teams.

### *4.3 Project Management*

4.3.1 Continuity of key personnel is required for duration of contract.

4.3.2 The Offeror must propose a predictive, performance-based (e.g., Earned Value Management System) method for tracking and reporting periodic status, cost, schedule, performance, activities, and variances. The Offeror's Earned Value Management System should meet ANSI/EIA Standard 748. Information on EVMS is available at <http://www.acq.osd.mil/pm>.

4.3.3 The Offeror must provide the TWIC Program office visibility of activities, schedule, risks, issues, personnel, labor hours, cost, etc. Deviations (between planned, actual, and budgeted) in cost, schedule, and performance must be identified in conjunction with weekly status reports delivered to the COTR for distribution to the TWIC Program Office.

4.3.4 The government anticipates using Primavera/TeamPlay® as the project management and Earned Value Management (EVM) tools. Offerors must ensure any and all internal project tracking tools used are compatible with Primavera/TeamPlay® and that associated schedules, documents, issues, risks, etc., can be imported by a novice user.

4.3.5 The Contractor must develop, and be prepared to execute, a transition plan and approach for three potential outcomes (decisions) resulting during or after Prototype

*4.3.5.1 Decision to begin full-scale implementation during, or immediately after Prototype*

*4.3.5.2 Decision to delay full-scale implementation pending analysis of results of Prototype and approval of DHS and Congress. This course of action is expected to require minimum sustainment of operations pending formal decision.*

*4.3.5.3 Decision to terminate or transfer responsibility for all Credentialing efforts during, or at the conclusion of Prototype*

### *4.4 Meetings*

4.4.1 Offeror will develop agendas and minutes for any meetings they request, and manage associated issues and action items to their resolution. This information must be provided with the Offeror's weekly status report delivered to the COTR.

***5 Deliverables and Schedule of Delivery ("days" = calendar days)***

***5.1 Before providing the final version of a deliverable, the Contractor must provide to the government (1) a brief approach and methodology, (2) initial outline, and then (3) initial draft for review. The Contractor must include these delivery milestones in their project schedules.***

| TASK # | DESCRIPTION | DELIVERABLES | TIMEFRAME |
|---|---|---|---|
| 1 | Planning | 1. Program Management Plan | CA + 10 days |
| | | 2. Primavera/TeamPlay® compliant Earned Value Management inputs | CA + 15 |
| | | 3. Site Survey | CA + 30 |
| | | 4. Documented Site Survey results | Site Survey + 5 days |
| | | 5. Weekly Status Report | Weekly |
| | | 6. Risk Management Plan (Consistent with TWIC PMO Risk Management Plan) | CA + 30 |
| | | 7. Quality Assurance Plan | CA + 45 days |
| | | 8. Configuration Management Plan | CA + 45 days |
| | | 9. Disaster Recovery/Continuity of Operations Plan | CDR + 60 |
| | | 10. Performance Metrics (methodology and format) | CA + 15 |
| | | 11. Performance Metrics (report) | Monthly (once local facilities are activated) |
| | | 12. Status Meetings | As Required |
| | | | |
| 2 | Design and Development | 13. Preliminary Design Review | CA + 25 days |
| | | 14. Critical Design Review | CA + 45 days |
| | | 15. Interface Design Documents | CDR + 20 days |

| | | | |
|---|---|---|---|
| | | 16. User Manual | CDR + 60 days |
| | | 17. Operations/System Administration Manual | CDR + 60 days |
| | | 18. Workflow Management System | CDR + 75 days |
| | | 19. Software Development Kits, Interfaces/APIs (as required for interfaces between Access Control Systems and TWIC Local Node) | CDR + 90 days |
| | | 20. Test scripts for IV&V Contractor | CDR + 5 days |
| | | 21. Periodic Meetings | As Required |
| | | 22. Weekly Status Report | Weekly |
| 3 | Installation and Training | 23. Standard Operating Procedures | CDR + 60 days |
| | | 24. Training Plan | CA + 45 days |
| | | 25. Trusted Agent Certification Plan | CA + 90 days |
| | | 26. Facility Certification Plan | CA + 90 days |
| | | 27. Prototype Solution hardware and software | CDR + 60 |
| | | 28. Equipment Inventory List | On-going (as procured and installed) |
| | | 29. Written Agreements with External Entities | Date TBD, but in advance of initial operations, or installations. |
| | | 30. Periodic meetings | As Required |
| | | 31. Weekly Status Reports | Weekly |

| | | | |
|---|---|---|---|
| 4 | Operations | 32. Help Desk support<br>33. Compatible products list<br>34. Operations and maintenance of proposed solution<br>35. IT support for proposed solution<br>36. User Surveys<br>37. Periodic Meetings<br>38. Weekly Status Report | On-going<br>CDR + 90<br>On-going<br>On-going<br>CA + 120<br>As Required<br>Weekly |
| | | | |
| 5 | Post-Prototype Support | 39. Transition Plan from Prototype to Implementation and estimated costs<br>40. Implementation Data Model<br>41. Prototype Report (see section 3.17 and 3.26)<br>42. Periodic Meetings | CA + 150<br>CDR + 90<br>CA + 180<br>As Required |
| 6 | Option 1<br>Prototype Phase Sustainment | 43. Status Report<br>44. Help Desk and Technical Support | Bi-Weekly<br>On-going |